

Amendments to the Claims

1. (Previously presented) A method for authenticating digital data in a system for writing digital data entered from an input device to a memory device and transferring the digital data written in the memory device to a receiving device, said method comprising the steps of:

performing a first device authentication between the input device and the memory device when writing digital data from the input device to the memory device; and

performing a second device authentication between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device.

2. (Previously presented) The method of claim 1 comprising the step of:

mixing data for performing device authentication into the digital data written from said input device to said memory device and the digital data transferred from said memory device to said receiving device.

3. (Previously presented) The method of claim 1 wherein said second device authentication is performed by a central processing unit built into said memory device.

4. (Previously presented) The method of claim 1 wherein said digital data is transferred as authenticated data if said first and second device authentications are successful and is transferred as ordinary data if said first and second device authentications are not successful.

5. (Previously presented) The method of claim 1 wherein said first device authentication is performed using a first encryption function and key and said second device authentication is performed using a second encryption function and key.

6. (Cancelled)

7. (Cancelled)

8. (Previously presented) The method of claim 1 wherein said device authentication between said input device and said memory device is performed by using a public key system.

9. (Cancelled)

10. (Previously presented) The method of claim 1 wherein each of said device authentications involves having a first device ascertain that a second device possesses a secret value corresponding to a value held by the first device.

11. (Previously presented) The method of claim 10 wherein the first device is a recipient of digital data from the second device.

12. (Previously presented) The method of claim 1 wherein each of said device authentications involves the exchange of an authentication value generated independently of said digital data.

13. (Previously presented) The method of claim 1, comprising the further steps, performed by the memory device, of:

generating an electronic signature on the digital data when writing the digital data from the input device to the memory device; and

authenticating the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

14. (Previously presented) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform the method steps of claim 1.

15. (Previously presented) Apparatus for authenticating digital data in a system for writing digital data entered from an input device to a memory device and transferring the digital data written in the memory device to a receiving device, said apparatus comprising:

means for performing a first device authentication between the input device and the memory device when writing digital data from the input device to the memory device; and

means for performing a second device authentication between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device.

16. (Previously presented) The apparatus of claim 15 wherein said means for performing said second device authentication comprises a central processing unit built into said memory device.

17. (Previously presented) The apparatus of claim 15 wherein said first device authentication is performed using a first encryption function and key and said second device authentication is performed using a second encryption function and key.

18. (Previously presented) The apparatus of claim 17 wherein said encryption functions and said first key are stored in a read-only memory of said memory device.

19. (Previously presented) The apparatus of claim 17 wherein said second key is encrypted and stored in NAND record space.

20. (Previously presented) The apparatus of claim 15, further comprising:
means associated with the memory device for generating an electronic signature on digital data when writing the digital data from the input device to the memory device; and
means associated with the memory device for authenticating the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

21. (Previously presented) A memory device for authenticating digital data in a system for writing digital data entered from an input device to the memory device and transferring the digital data written in the memory device to a receiving device, said memory device comprising:
means for performing a first device authentication with the input device when writing digital data from the input device; and

means for performing a second device authentication with the receiving device when transferring the digital data to the receiving device.

22. (Previously presented) The memory device of claim 21, further comprising:
means for generating an electronic signature on the digital data when writing the digital data from the input device to the memory device; and
means for authenticating the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

B1
23-29. (Cancelled)

30. (Currently amended) The memory device of claim 26 A memory device for authenticating digital data in a system for writing digital data entered from an input device to the memory device and transferring the digital data written in the memory device to a receiving device, said memory device comprising:
means for generating an electronic signature on digital data when writing the digital data from the input device;
means for storing the digital data and the electronic signature; and
means for authenticating the electronic signature on the digital data when transferring the digital data to the receiving device, wherein said memory device is a flash memory and stores said electronic signature on said digital data in a redundant area not to be calculated by an ECC of each page in a memory area.